CRITICAL FAULT

PROFESSIONALLY PARANOID

PHYSICAL SECURITY

Physical Security is an underappreciated aspect of a company's cybersecurity architecture. Physical security risks such as unauthorized access to server rooms or employee hardware can circumvent traditional digital protection methods. A company's physical security controls, practices, and procedures should be considered an integral part of any cybersecurity policies.

Physical Security vulnerabilities should never be ignored. Just like ignoring a network vulnerability opens up your organization to cyber attacks, leaving your perimeter under-protected could lead to data exposures, malware attacks, or unauthorized eavesdroppers.

CRITICAL FAULT

PROFESSIONALLY PARANOID

THREAT VECTORS

Protecting your organization's perimeter should be top priority. The first step to protecting your company is identifying areas of your critical infrastructure that need to be improved. Various Threat Vectors impact what security controls you need to have in place.

EXTERIOR ENTRY POINTS

A building's exterior entry points are the most important part of a physical security system, with some of the most robust systems being implemented. However, it can be easy to miss vulnerabilities when building a system without having an adversarial thought process present during the design.

Critical Fault identifies these vulnerabilities and provides suggestions for improvement.

DEVICE IMPLANTATION

Attackers will often try to administer malware through infected devices. The attacker leaves an infected USB drive in a lobby, parking lot, or other organizational watering hole hoping someone will plug in the device. Once plugged in, the device begins secretly installing malicious software onto the infected system.

Additionally, if a threat actor gains unauthorized access to the building, they can implant the device directly into organizational systems themselves.

CRITICAL FAULT

PROFESSIONALLY PARANOID

THREAT VECTORS

It is possible for attackers to circumvent digital protections by gaining direct access to physical assets. Critical Fault analyzes your organization's physical security controls to ensure that your critical infrastructure is protected.

POINTS OF EXIT

Access controls at entrances are often the first line of defense and the strongest, however, access controls for exiting the building are just as critical. Once an attacker gains access to a building, they are often met with little to no resistance from security controls.

Critical Fault analyzes points of exit and identifies any vulnerabilities to help your company protect itself from a threat actor.

SOCIAL ENGINEERING

Human behavior can be exploited to gain access to controlled areas. Threat actors will often try to deceive an organization's employees into believing the actor belongs. Intruders have been known to disguise themselves as contractors, impersonate employees, or slip into sensitive areas by "tailgating" behind authorized employees.

Critical Fault's security experts stay up-to-date on the latest social engineering trends to help keep your employees trained and security aware.

CRITICAL FAULT

PROFESSIONALLY PARANOID

PHYSICAL CONTROLS

ACCESS CONTROLS

Including security staff, proper lighting, fences, doors, locks, scanners, ID's, security guards, keys, etc.

VIDEO SURVEILLANCE

Including CCTV, Centralized and Decentralized IP cameras, etc.

INTRUSION DETECTION

Including intrusion detection systems, network oversight, host monitoring, anomaly detection, signature-based detection

Aside from assessing your organization's physical controls, Critical Fault augments it's assessments by providing the following:

EMPLOYEE AND MANAGEMENT TRAINING

Train staff to understand physical security best practices and how to avoid common physical security mistakes.

EQUIPMENT DOCUMENTATION

Documentation of all security controls in place and asset inventories to discover any missing or additional devices.